Welcome to the PIA for FY 2010!

Congress passed the E-Government Act of 2002 to encourage the use of Web-based Internet applications or other information technology by Government agencies, with the intention of enhancing access to government information and services and increasing the effectiveness, efficiency, and quality of government operations.

To combat public concerns regarding the disclosure of private information, the E-Government Act mandated various measures, including the requirement that Federal agencies conduct a Privacy Impact Assessment (PIA) for projects with information technology systems that collect, maintain, and/or disseminate "personally identifiable information" of the public. Personally identifiable information, or "personal information," is information that may be used to identify a specific person.

The Privacy Act and VA policy require that personally identifiable information only be used for the purpose(s) for which it was collected, unless consent (opt-in) is granted. Individuals must be provided an opportunity to provide consent for any secondary use of information, such as use of collected information for marketing.

Directions:

VA 6508 is the directive which outlines the PIA requirement for every System/Application/Program. More information can be found by reading VA 6508.

If you find that you can't click on checkboxes, make sure that you are: 1) Not in "design mode" and 2) you have enabled macros.

PIA Website: http://vaww.privacy.va.gov/PIA.asp

Roles and Responsibilities:

Roles and responsibilities for the specific process are clearly defined for all levels of staff in the Privacy Impact Assessment Handbook 6202.2 referenced in the procedure section of this document.

a. The Privacy Officer is responsible for the overall coordination and review of the PIA to ensure compliance with VA Handbook 6202.2.

b. Records Officer is responsible for supplying records retention and deletion schedules.

c. Information Technology (IT) staff responsible for the privacy of the system data will perform a PIA in accordance with VA Handbook 6202.2 and to immediately report all anomalies to the Privacy Service and appropriate management chain.

d. Information Security Officer (ISO) is responsible for assisting the Privacy Officer and providing information regarding security controls.

e. The CIO is responsible for ensuring that the systems under his or her jurisdiction undergo a PIA. This responsibility includes identifying the IT systems; coordinating with the Privacy Officer, Information Security Officer, and others who have concerns about privacy and security issues; and reviewing and approving the PIA before submission to the Privacy Service.

Definition of PII (Personally Identifiable Information)

Information in identifiable form that is collected and stored in the system that either directly identifies and individual by name, address, social security number, telephone number, e-mail address, biometric identifiers, photograph, or other unique numbers, codes or characteristics or combined, indirect indentify an individual such as a combination of gender, race, birth date, geographical indicators, license number is also considered PII.

Macros Must Be Enabled on This Form

To enable macros, go to: 1) Tools > Macros > Security - Set to Medium; 2) Click OK; 3) Close the file and when reopening click on Enable Macros at the prompt.

(FY 2010) PIA: System Identification

Program or System Name:	Ann Arbor VA Healthcare System – VistA Legacy
OMB Unique System / Application / Program Identifier (AKA: UPID #):	029-00-01-11-01-1180-00
Description of System / Application / Program:	The VistA-Legacy system is the software platform and hardware infrastructure (associated with clinical operations) on which the VHA health care facilities operate their software applications and support for E-Government initiatives. It includes the computer equipment associated with clinical operations and the employees (approximately 2500 FTE) necessary to operate the system. VistALegacy is a client-server system. It links the facility computer network to over 100 applications and databases. In 2006, the VistA-Legacy system supported IT services across the VA organization which had a network of 21 Veterans Integrated Service Networks (VISNs) that managed 155 medical centers, over 881 community based outpatient clinics, 46 residential rehabilitation treatment programs, 135 nursing homes, 207 readjustment counseling centers, 57 veteran benefits regional offices, and 125 national cemeteries. VistA-Legacy provides critical data that supports the delivery of healthcare to veterans and their dependants. Using the computer, the VA health care provider can access VistA-Legacy applications and meet a wide range of health care data needs. The VistA-Legacy system operates in medical centers, ambulatory and community-based clinics, nursing homes and domiciliary. The VistA-Legacy system is in the mature phase of the capital investment lifecycle.
Facility Name:	VA Ann Arbor Healthcare System

Title:	Name:	Phone:	Email:
Privacy Officer:	Sandra Kidd	734-845-5314	sandra.kidd@va.gov
Information Security Officer:	Mark Latendresse	734-845-5351	mark.latendresse@va.gov
Chief Information Officer:	Ronald Wuthrich	734-845-5733	ronald.wuthrich@va.gov
Person Completing Document:	John M Wilkerson	734-845-5563	john.wilkerson@va.gov
System Manager	Richard Ray	734-845-3960	richard.ray@va.gov
Information Security Officer:	Jason Brown	734-845-5802	jason.brown4@va.gov
Chief Information Systems:	Rob Whitehurst	734-845-5729	rob.whitehurst@va.gov

Date of Last PIA Approved by VACO Privacy Services: (MM/YYYY)	06/2008
Date Approval To Operate Expires:	06/2011
What specific legal authorities authorize this program or system:	Title 38, United States Code, Section 7301(a)
What is the expected number of individuals that will have their PII stored in this system:	1,000,000-9,999,999

Identify what stage the System / Application / Program is at:	Operations/Maintenance
The approximate date (MM/YYYY) the system will be operational (if in the Design or Development stage), or the approximate number of years the system/application/program has been in operation.	Operational now for over 25 years.
Is there an authorized change control process which documents any changes to existing applications or systems?	Yes
If No, please explain:	
Has a PIA been completed within the last three years?	Yes
Date of Report (MM/YYYY):	

Please check the appropriate boxes and continue to the next TAB and complete the remaining questions on this form.

- ☑ Have any changes been made to the system since the last PIA?
- ☑ Is this a PIV system/application/program collecting PII data from Federal employees, contractors, or others performing work for the VA?
- ☑ Will this system/application/program retrieve information on the basis of name, unique identifier, symbol, or other PII data?
- ☑ Does this system/application/program collect, store or disseminate PII/PHI data?
- ☑ Does this system/application/program collect, store or disseminate the SSN?

If there is no Personally Identifiable Information on your system , please skip to TAB 12. (See Comment for Definition of PII)

(FY 2010) PIA: System of Records

Is the data maintained under one or more approved System(s) of Records?	Yes
if the answer above is no, please skip to row 16.	
For each applicable System(s) of Records, list:	
1. All System of Record Identifier(s) (number):	79VA19
2. Name of the System of Records:	Veterans Health Information System and Technology Architecture (VISTA)-VA
3. Location where the specific applicable System of Records Notice may be accessed (include the URL):	http://vaww.vhaco.va.gov/privacy/SystemofRecords.htm
Have you read, and will the application, system, or program comply with, all data management practices in the System of Records Notice(s)?	Yes
Does the System of Records Notice require modification or updating?	No
	(Please Select Yes/No)
Is PII collected by paper methods?	Yes
Is PII collected by verbal methods?	Yes
Is PII collected by automated methods?	Yes
Is a Privacy notice provided?	Yes
Proximity and Timing: Is the privacy notice provided at the time of data collection?	Yes
Purpose: Does the privacy notice describe the principal purpose(s) for which the information will be used?	Yes
Authority: Does the privacy notice specify the effects of providing information on a voluntary basis?	Yes
Disclosures: Does the privacy notice specify routine use(s) that may be made of the information?	Yes

(FY 2010) PIA: Notice

Please fill in each column for the data types selected.

Data Type	Collection Method	What will the subjects be told about the information collection?	How is this message conveyed to them?	How is a privacy notice provided?
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	ALL	The most common data types that are captured and accessed on a regular basis by authorized individuals are first and last name, middle initial, DOB, SSN, and address. This patient information falls into two classes: administrative and clinical. Clinical information is used to diagnose, prescribe treatment and follow clinically the patient through his/her health care encounters. Administrative data is used to identify the veteran (SSN), correspond to/from (name and address), determine eligibility (patient administrative info and SSA and IRS data), enter Next of Kin and emergency contact information and collect insurance information.	All	All
Family Relation (spouse, children, parents, grandparents, etc)	ALL	The most common data types that are captured and accessed on a regular basis by authorized individuals are first and last name, middle initial, DOB, SSN and address. Dependent data is utilized to determine eligibility for VA benefits. In addition, NOK and emergency contact information is often a dependent of the veteran and this data is used in case of emergency or need during the patient's episode of care.	All	All
Service Information	ALL	Military Service Information (Branch of service, discharge date, discharge type, service connection rating, medical conditions related to military service, etc). This information is collected to assess eligibility for VA healthcare benefits, type of healthcare needed.	All	All

Medical Information	ALL	VistA-Legacy applications and meet a wide range of health care data needs. The VistA-Legacy system operates in medical centers, ambulatory and community-based clinics, nursing homes and domiciliary, and thus collects a wide range of personal medical information for clinical diagnosis, treatment, patient evaluation, and patient care. Common types of personal medical information would include lab test results, prescriptions, allergies, medical diagnoses, vital signs, etc. The information is used to treat and care for the veteran patient. Clinical information from VA and DoD is used in the diagnosis and treatment of the veteran (Health Data Repository).	All	All
Criminal Record Information	ALL	Specific information is not input into the VistA system but the fugitive felon program includes a flag on the patient file identifying the need to contact the VA police.	All	All
Guardian Information	ALL	Next of kin, DNR instructions, health care proxy designation. This information is used in the notification process and as required for medical decisions. Guardian information is often flagged in the medical record to ensure the timely and appropriate notification during healthcare decision making from provider/patient/guardian.	All	All
Education Information	ALL	Used to develop treatment plans that are understandable to patient's educational level.	All	All
Benefit Information	ALL	Used to review/update benefit coverage for use in billing for care.	All	All
Other (Explain)				

Data Type	Is Data Type Stored on your system?	Source (If requested, identify the specific file, entity and/or name of agency)	Is data collection Mandatory or Voluntary?	Additional Comments
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	Yes	Veteran	Mandatory	

Family Relation (spouse, children, parents, grandparents, etc)	Yes	Veteran	Mandatory
Service Information	Yes	Veteran	Mandatory
Medical Information	Yes	Veteran	Mandatory
Criminal Record Information	Yes	Veteran	Mandatory
Guardian Information	Yes	Veteran	Mandatory
Education Information	Yes	Veteran	Mandatory
Benefit Information	Yes	Veteran	Mandatory
Other (Explain)			
Other (Explain)			
Other (Explain)			

(FY 2010) PIA: Data Sharing

Organization	Name of Agency/Organization	Do they access this system?	Identify the type of Data Sharing and its purpose.	Is PII or PHI Shared?	What is the procedure you reference for the release of information?
Internal Sharing: VA Organization	Local Vet Center, VBA and Health Eligibility Center, Service Officers.	Yes	Health and Demographic Information is shared with the local Vet Center and VBA and Health Eligibility Center. Vet Center and the medical center shares patient health information and demographic information as they work closely to develop the overall care and services for the veteran. Comp and Pen information (health and admin) is required to be shared with the VBA to process these veteran's request for service reviews for disability.	Both PII & PHI	Individuals must visit the VAMC where they receive their care and begin the release of information process which includes being informed of privacy rules and the Freedom of Information Act (FOIA). The facility is required to obtain the signature from the veteran on the release of information form (10-5345). Picture ID from the individual is required for proof of identity. Information is entered into the ROI package and tracked. Data is released as indicated once all steps are completed.
Other Veteran Organization	State Veterans Home	No	On limited occasions we need to supply health and demographic information on patients to the State Veterans Home for continuity of care when a patient is transferred to their care. The State Home Program is a partnership between the U.S. Department of Veterans Affairs and the States to construct or acquire nursing home, domiciliary and/or adult day health care facilities. Hospital care may be included when provided in conjunction with nursing home or domiciliary care. VA participates in these five grant-in-aid programs for States. VA may participate in up to 65 percent of the cost of construction or acquisition of State nursing homes or domiciliary or for renovations to existing State homes. VA also provides per diem payments to States for the care of eligible veterans in State homes. A State home is owned and operated by a State. VA assures Congress that State homes provide quality care through inspections, audits, and reconciliation of records conducted by the VA medical center of jurisdiction.	Both PII & PHI	Individuals must visit the VAMC where they receive their care and begin the release of information process which includes being informed of privacy rules and the Freedom of Information Act (FOIA). The facility is required to obtain the signature from the veteran on the release of information form (10-5345). Picture ID from the individual is required for proof of identity. Information is entered into the ROI package and tracked. Data is released as indicated once all steps are completed.

Other Federal Government Agency	IRS, DOD, CDC	Yes	Name, SSN, DOB, and Sex are transmitted to SSA and the SSN and first four characters of the surname are transmitted to IRS in order to verify certain veteran's self-reported income information with federal tax information to identify veteran's responsibility for making medical care co-payments and enhance revenue from first party collections (Income Verification Match). Also, veteran information is commonly shared with the Department of Defense (DoD). There is certain VHA VistA patient data that is shared with DoD through the Federal/Bidirectional Health Information Exchange (FHIE/BHIE) Program under DUAs that have been in effect for several years. In addition, certain clinical information is being shared with CDC, also under an established national DUA. It is every agencies responsibility to protect the data that is shared between organizations.	Both PII & PHI	Individuals must visit the VAMC where they receive their care and begin the release of information process which includes being informed of privacy rules and the Freedom of Information Act (FOIA). The facility is required to obtain the signature from the veteran on the release of information form (10-5345). Picture ID from the individual is required for proof of identity. Information is entered into the ROI package and tracked. Data is released as indicated once all steps are completed.
State Government Agency	State Veterans Home	No	On limited occasions we need to supply health and demographic information on patients to the State Veterans Home for continuity of care when a patient is transferred to their care. The State Home Program is a partnership between the U.S. Department of Veterans Affairs and the States to construct or acquire nursing home, domiciliary and/or adult day health care facilities. Hospital care may be included when provided in conjunction with nursing home or domiciliary care. VA participates in these five grant-in-aid programs for States. VA may participate in up to 65 percent of the cost of construction or acquisition of State nursing homes or domiciliary or for renovations to existing State homes. VA also provides per diem payments to States for the care of eligible veterans in State homes. A State home is owned and operated by a State. VA assures Congress that State homes provide quality care through inspections, audits, and reconciliation of records conducted by the VA medical center of jurisdiction.	Both PII & PHI	Individuals must visit the VAMC where they receive their care and begin the release of information process which includes being informed of privacy rules and the Freedom of Information Act (FOIA). The facility is required to obtain the signature from the veteran on the release of information form (10-5345). Picture ID from the individual is required for proof of identity. Information is entered into the ROI package and tracked. Data is released as indicated once all steps are completed.
Local Government Agency					
Research Entity					

Other Project / System	DOD, CDC.	No	There is certain VHA VistA health and demographic patient data that is shared with DoD through the Federal/Bidirectional Health Information Exchange (FHIE/BHIE) Program under DUAs that have been in effect for several years. In addition, certain clinical information is being shared with CDC, also under an established DUA. Billing information is sent to various insurance companies.	Both PII & PHI	Individuals must visit the VAMC where they receive their care and begin the release of information process which includes being informed of privacy rules and the Freedom of Information Act (FOIA). The facility is required to obtain the signature from the veteran on the release of information form (10-5345). Picture ID from the individual is required for proof of identity. Information is entered into the ROI package and tracked. Data is released as indicated once all steps are completed.
Other Project / System					
Other Project / System					

(FY 2010) PIA: Access to Records

Does the system gather information from another system?	Yes
Please enter the name of the system:	Health Data Repository (VA and DOD), other VA Medical Centers.
Per responses in Tab 4, does the system gather information from an individual?	Yes
If information is gathered from an individual, is the information provided:	☑ Through a Written Request ☑ Submitted in Person ☑ Online via Electronic Form
Is there a contingency plan in place to process information when the system is down?	Yes

(FY 2010) PIA: Secondary Use

Will PII data be included with any secondary use request?	No
if yes, please check all that apply:	☐ Drug/Alcohol Counseling ☐ Mental Health ☐ HIV ☐ Research ☐ Sickle Cell ☐ Other (Please Explain)

Describe process for authorizing access
to this data.
Answer:

(FY 2010) PIA: Program Level Questions

Does this PIA form contain any sensitive information that could cause harm to the Department of Veterans Affairs or any party if disclosed to the public? If Yes, Please Specify:	No
Explain how collected data are limited to required elements: Answer:	Data is collected electronically based on the automation of VA Forms and clinical procedures.
How is data checked for completeness? Answer:	Validation of data is reviewed by intake and data analysis staff and compared to paper forms and there are automated system checks for registrations and verified with Next of Kin. Internal Audits are conducted on data for completeness and timeliness.
What steps or procedures are taken to ensure the data remains current and not out of date? Answer:	Clinical data is reviewed and updated in the patient record at each visit and is electronically signed by the author. Administrative data is updated annually with each application for care and at each patient visit.
How is new data verified for relevance, authenticity and accuracy? Answer:	New data is compared with printed form via patient verification, signed official forms. (birth certificate, SS cards, Picture ID, Driver license, etc.)
Additional Information: (Provide any necessary clarifying information or additional explanation for this section.) Answer:	

(FY 2010) PIA: Retention & Disposal

What is the data retention period? Answer:	Clinical information is retained in accordance with VA Records Control Schedule 10-1. Demographic information is updated as applications for care are submitted and retained in accordance with VA Records Control Schedule 10-1.
Explain why the information is needed for the indicated retention period? Answer:	

	Electronic Final Version of Patient Medical Record is destroyed/deleted 75 years after the last episode of patient care as instructed in VA Records Control Schedule 10-1, Item XLIII, 2.b. (Page190). At the present time, VistA Imaging retains all images. We are performing a study to explore whether some images can be eliminated on an earlier schedule. Electronic Final Version of Patient Medical Record is destroyed/deleted 75 years after the last episode of patient care as instructed in VA Records Control Schedule 10-1, Item XLIII, 2.b. (Page190). At the present time, VistA Imaging retains all images. We are performing a study to explore whether some images can be eliminated on an earlier schedule.
What are the procedures for eliminating data at the end of the retention period? Answer:	
Where are these procedures documented? Answer:	VA Handbook 6300; Record Control Schedule 10-1
How are data retention procedures enforced? Answer:	Procedures will be enforced using technical and managerial control mechanisms. Access privileges and business rules control various roles at our site and are closely monitored VA Records Control Schedule 10-1 (page 8): Records Management Responsibilities: The Health Information Resources Service (HIRS) is responsible for developing policies and procedures for effective and efficient records management throughout VHA. In addition, HIRS acts as the liaison between VHA and National Archives and Records Administration (NARA) on issues pertaining to records management practices and procedures. Field records officers are responsible for records management activities at their facilities. Program officials are responsible for creating, maintaining, protecting, and disposing of records in their program area in accordance with NARA regulations and VA policy. All VHA employees are responsible to ensure that records are created, maintained, protected, and disposed of in accordance with NARA regulations and VA policies and procedures. Disposition of Records at our site are in accordance with NARA regulation.
Has the retention schedule been approved by the National Archives and Records Administration (NARA)	Yes
Additional Information: (Provide any necessary clarifying information or additional explanation for this section.)	

Answer:

(FY 2010) PIA: Children's Online Privacy Protection Act (COPPA)

Will information be collected through the internet from children under age 13?	No

If Yes, How will parental or guardian approval be obtained?

Answer:

(FY 2010) PIA: Security

Is the system/application/program following IT security Requirements and procedures required by federal law and policy to ensure that information is appropriately secured.	Yes
Has the system/application/program conducted a risk assessment, identified appropriate security controls to protect against that risk, and implemented those controls..	Yes
Is security monitoring conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information?	Yes
Is security testing conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information?	Yes
Are performance evaluations conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information?	Yes
If 'No' to any of the 3 questions above, please describe why: Answer:	
Is adequate physical security in place to protect against unauthorized access?	Yes
If 'No' please describe why: Answer:	
Explain how the project meets IT security requirements and procedures required by federal law. Answer:	The facility follows the Office of Cyber & Information Security (OCIS) established directives, policies, & procedures which are consistent with the provisions of Federal Information Security Management Act (FISMA) as well as guidance issued by the Office of Management & Budget (OMB), the National Institute of Standards & Technology (NIST), & other requirements that VistA-Legacy is and has been subject to. Locally, each system is subjected to a security control check list which is implemented prior to a system being placed into service and it is the responsibility of the system manager with oversight by the ISO and CIO. Each checklist is reviewed during the Change Control Board meetings, which is chaired by the CIO no third party software is introduced without being tested and approved by CCB. Any new system must be approved on the IT procurement website which includes documentation and security review before concurrence. All projects which include medical devices go through the local equipment committee which both the ISO and CIO are members. Medical Device security reviews must include the check list that is supplied with VA Directive 6550 before purchase. At the end of the life cycle of the project any data contained on hardware/equipment is mandated to be sanitized via the approved VA method. An IT specialist is required to be a member of any team at

Explain what security risks were identified in the security assessment? *(Check all that apply)*

- [x] Air Conditioning Failure
- [x] Chemical/Biological Contamination
- [ ] Blackmail
- [x] Bomb Threats
- [x] Cold/Frost/Snow
- [x] Communications Loss
- [x] Computer Intrusion
- [x] Data Destruction
- [ ] Data Disclosure
- [x] Data Integrity Loss
- [x] Denial of Service Attacks
- [ ] Earthquakes
- [x] Eavesdropping/Interception
- [x] Fire (False Alarm, Major, and Minor)
- [x] Flooding/Water Damage
- [x] Hardware Failure
- [x] Malicious Code
- [x] Computer Misuse
- [x] Power Loss
- [x] Sabotage/Terrorism
- [x] Storms/Hurricanes
- [ ] Substance Abuse
- [x] Theft of Assets
- [x] Theft of Data
- [x] Vandalism/Rioting
- [x] Errors (Configuration and Data Entry)
- [x] Burglary/Break In/Robbery
- [x] Identity Theft
- [x] Fraud/Embezzlement

Answer: (Other Risks)

Explain what security controls are being used to mitigate these risks. *(Check all that apply)*

- [x] Risk Management
- [x] Access Control
- [x] Awareness and Training
- [x] Contingency Planning
- [x] Physical and Environmental Protection
- [x] Personnel Security
- [x] Certification and Accreditation Security Assessments
- [x] Audit and Accountability
- [x] Configuration Management
- [x] Identification and Authentication
- [x] Incident Response
- [x] Media Protection

Answer: (Other Controls)

PIA: PIA Assessment

Identify what choices were made regarding the project/system or collection of information as a result of performing the PIA.

Answer: VistA-Legacy is a steady state project and is governed by existing policies and procedures. Due to this and the completion and review of this PIA, no modifications are required.

Availability Assessment: If the data being collected is not available to process for any reason what will the potential impact be upon the system or organization? **(Choose One)**	☑	The potential impact is **high** if the loss of availability could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals.
	☐	The potential impact is **moderate** if the loss of availability could be expected to have a serious adverse effect on operations, assets or individuals.
	☐	The potential impact is **low** if the loss of availability could be expected to have a limited adverse effect on operations, assets or individuals.
Integrity Assessment: If the data being collected has been corrupted for any reason what will the potential impact be upon the system or organization? **(Choose One)**	☑	The potential impact is **high** if the loss of availability could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals.
	☐	The potential impact is **moderate** if the loss of availability could be expected to have a serious adverse effect on operations, assets or individuals.
	☐	The potential impact is **low** if the loss of availability could be expected to have a limited adverse effect on operations, assets or individuals.
Confidentiality Assessment: If the data being collected has been shared with unauthorized individuals what will the potential impact be upon the system or organization? **(Choose One)**	☑	The potential impact is **high** if the loss of availability could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals.
	☐	The potential impact is **moderate** if the loss of availability could be expected to have a serious adverse effect on operations, assets or individuals.
	☐	The potential impact is **low** if the loss of availability could be expected to have a limited adverse effect on operations, assets or individuals.

The controls are being considered for the project based on the selections from the previous assessments?

The minimum security requirements for our high impact system cover seventeen security-related areas with regard to protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems. The security-related areas include: access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity. Our facility employs all security controls in the respective high impact security control baseline unless specific exceptions have been allowed based on the tailoring guidance

Please add additional controls:

(FY 2010) PIA: Additional Comments

Add any additional comments on this tab for any question in the form you want to comment on.
Please indicate the question you are responding to and then add your comments.

(FY 2010) PIA: VBA Minor Applications										
	Explain what minor application that are associated with your installation? *(Check all that apply)*									
		Records Locator System		Education Training Website		Appraisal System		Baker System		Veterans Assistance Discharge System (VADS)
		Veterans Assistance Discharge System (VADS)		VR&E Training Website		Web Electronic Lender Identification	X	Dental Records Manager		VBA Training Academy
		LGY Processing		VA Reserve Educational Assistance Program		CONDO PUD Builder		Sidexis		Veterans Service Network (VETSNET)
		Loan Service and Claims		Web Automated Verification of Enrollment		Centralized Property Tracking System	X	Priv Plus		Waco Indianapolis, Newark, Roanoke, Seattle (WINRS)
		LGY Home Loans		Right Now Web		Electronic Appraisal System	X	Mental Health Asisstant		BIRLS
		Search Participant Profile (SPP)		VA Online Certification of Enrollment (VA-ONCE		Web LGY	X	Telecare Record Manager		Centralized Accounts Receivable System (CARS)
		Control of Veterans Records (COVERS)		Automated Folder Processing System (AFPS)		Access Manager	X	Omnicell		Compensation & Pension (C&P)
		SHARE		Personal Computer Generated Letters (PCGL)		SAHSHA	X	Powerscribe Dictation System		Corporate Database
		Modern Awards Process Development (MAP-D)		Personnel Information Exchange System (PIES)		VBA Data Warehouse		EndoSoft		Control of Veterans Records (COVERS)
		Rating Board Automation 2000 (RBA2000)		Rating Board Automation 2000 (RBA2000)		Distribution of Operational Resources (DOOR)		Compensation and Pension (C&P)		Data Warehouse
		State of Case/Supplemental (SOC/SSOC)		SHARE		Enterprise Wireless Messaging System (Blackberry)		Montgomery GI Bill		INS - BIRLS
		Awards		State Benefits Reference System		VBA Enterprise Messaging System		Vocational Rehabilitation & Employment (VR&E) CH 31		Mobilization
		Financial and Accounting System (FAS)		Training and Performance Support System (TPSS)		LGY Centralized Fax System		Post Vietnam Era educational Program (VEAP) CH 32		Master Veterans Record (MVR
		Eligibility Verification Report (EVR)		Veterans Appeals Control and Locator System (VACOLS)		Review of Quality (ROQ)		Spinal Bifida Program Ch 18		BDN Payment History
		Automated Medical Information System (AMIS)290		Veterans On-Line Applications (VONAPP)		Automated Sales Reporting (ASR)		C&P Payment System		
		Web Automated Reference Material System (WARMS)		Automated Medical Information Exchange II (AIME II)		Electronic Card System (ECS)		Survivors and Dependents Education Assistance CH 35		
		Automated Standardized Performace Elements Nationwide (ASPEN)		Committee on Waivers and Compromises (COWC)		Electronic Payroll Deduction (EPD)		Reinstatement Entitelment Program for Survivors (REAPS)		
		Inquiry Routing Information System (IRIS)		Common Security User Manager (CSUM)		Financial Management Information System (FMI)		Educational Assistance for Members of the Selected Reserve Program CH 1606		
		National Silent Monitoring (NSM)		Compensation and Pension (C&P) Record Interchange (CAPRI)		Purchase Order Management System (POMS)		Reserve Educational Assistance Program CH 1607		
		Web Service Medical Records (WebSMR)		Control of Veterans Records (COVERS)		Veterans Canteen Web		Compensation & Pension Training Website		
		Systematic Technical Accuracy Review (STAR)		Corporate Waco, Indianapolis, Newark, Roanoke, Seattle (Corporate WINRS)		Inventory Management System (IMS)		Web-Enabled Approval Management System (WEAMS)		
		Fiduciary STAR Case Review		Fiduciary Beneficiary System (FBS)		Synquest		FOCAS		
		Veterans Exam Request Info System (VERIS)		Hearing Officer Letters and Reports System (HOLAR)		RAI/MDS		Work Study Management System (WSMS)		
		Web Automated Folder Processing System (WAFPS)		Inforce	X	ASSISTS		Benefits Delivery Network (BDN)		
		Courseware Delivery System (CDS)		Awards	X	MUSE	X	Personnel and Accounting Integrated Data and Fee Basis (PAID)		
		Electronic Performance Support System (EPSS)		Actuarial		Bbraun (CP Hemo)		Personnel Information Exchange System (PIES)		
		Veterans Service Representative (VSR) Advisor		Insurance Self Service	X	VIC		Rating Board Automation 2000 (RBA2000)		
		Loan Guaranty Training Website		Insurance Unclaimed Liabilities	X	BCMA Contingency Machines		SHARE		
		C&P Training Website		Insurance Online	X	Script Pro		Service Member Records Tracking System		

(FY 2010) PIA: VISTA Minor Applications										
	Explain what minor application that are associated with your installation? *(Check all that apply)*									
	X	ACCOUNTS RECEIVABLE	X	DRUG ACCOUNTABILITY	X	INPATIENT MEDICATIONS	X	OUTPATIENT PHARMACY	X	SOCIAL WORK
		ADP PLANNING (PLANMAN)	X	DSS EXTRACTS		INTAKE/OUTPUT	X	PAID	X	SPINAL CORD DYSFUNCTION
	X	ADVERSE REACTION TRACKING		EDUCATION TRACKING	X	INTEGRATED BILLING	X	PATCH MODULE	X	SURGERY
	X	ASISTS		EEO COMPLAINT TRACKING		INTEGRATED PATIENT FUNDS	X	PATIENT DATA EXCHANGE		SURVEY GENERATOR
	X	AUTHORIZATION/SUBSCRIPTION	X	ELECTRONIC SIGNATURE		INTERIM MANAGEMENT SUPPORT		PATIENT FEEDBACK	X	TEXT INTEGRATION UTILITIES
	X	AUTO REPLENISHMENT/WARD STOCK	X	ENGINEERING	X	KERNEL		PATIENT REPRESENTATIVE	X	TOOLKIT
		AUTOMATED INFO COLLECTION SYS	X	ENROLLMENT APPLICATION SYSTEM	X	KIDS	X	PCE PATIENT CARE ENCOUNTER		UNWINDER
	X	AUTOMATED LAB INSTRUMENTS	X	EQUIPMENT/TURN-IN REQUEST	X	LAB SERVICE		PCE PATIENT/IHS SUBSET		UTILIZATION MANAGEMENT ROLLUP
	X	AUTOMATED MED INFO EXCHANGE	X	EVENT CAPTURE		LETTERMAN	X	PHARMACY BENEFITS MANAGEMENT	X	UTILIZATION REVIEW
	X	BAR CODE MED ADMIN		EVENT DRIVEN REPORTING	X	LEXICON UTILITY	X	PHARMACY DATA MANAGEMENT	X	VA CERTIFIED COMPONENTS - DSSI
	X	BED CONTROL	X	EXTENSIBLE EDITOR		LIBRARY	X	PHARMACY NATIONAL DATABASE	X	VA FILEMAN
	X	BENEFICIARY TRAVEL		EXTERNAL PEER REVIEW	X	LIST MANAGER		PHARMACY PRESCRIPTION PRACTICE	X	VBECS
	X	CAPACITY MANAGEMENT - RUM	X	FEE BASIS	X	MAILMAN	X	POLICE & SECURITY	X	VDEF
	X	CAPRI		FUNCTIONAL INDEPENDENCE	X	MASTER PATIENT INDEX VISTA	X	PROBLEM LIST	X	VENDOR - DOCUMENT STORAGE SYS
	X	CAPACITY MANAGEMENT TOOLS		GEN. MED. REC. - GENERATOR	X	MCCR NATIONAL DATABASE		PROGRESS NOTES		VHS&RA ADP TRACKING SYSTEM
	X	CARE MANAGEMENT		GEN. MED. REC. - I/O	X	MEDICINE	X	PROSTHETICS	X	VISIT TRACKING
	X	CLINICAL CASE REGISTRIES		GEN. MED. REC. - VITALS	X	MENTAL HEALTH		QUALITY ASSURANCE INTEGRATION	X	VISTALINK
	X	CLINICAL INFO RESOURCE NETWORK		GENERIC CODE SHEET		MICOM		QUALITY IMPROVEMENT CHECKLIST		VISTALINK SECURITY
		CLINICAL MONITORING SYSTEM		GRECC	X	MINIMAL PATIENT DATASET	X	QUASAR	X	VISUAL IMPAIRMENT SERVICE TEAM ANRV
	X	CLINICAL PROCEDURES	X	HEALTH DATA & INFORMATICS	X	MYHEALTHEVET	X	RADIOLOGY/NUCLEAR MEDICINE		VOLUNTARY TIMEKEEPING
	X	CLINICAL REMINDERS	X	HEALTH LEVEL SEVEN		Missing Patient Reg (Original) A4EL	X	RECORD TRACKING		VOLUNTARY TIMEKEEPING NATIONAL
	X	CMOP	X	HEALTH SUMMARY	X	NATIONAL DRUG FILE	X	REGISTRATION	X	WOMEN'S HEALTH
	X	CONSULT/REQUEST TRACKING	X	HINQ		NATIONAL LABORATORY TEST	X	RELEASE OF INFORMATION - DSSI		CARE TRACKER
	X	CONTROLLED SUBSTANCES	X	HOSPITAL BASED HOME CARE		NDBI	X	REMOTE ORDER/ENTRY SYSTEM		
		CPT/HCPCS CODES	X	ICR - IMMUNOLOGY CASE REGISTRY	X	NETWORK HEALTH EXCHANGE	X	RPC BROKER		
		CREDENTIALS TRACKING	X	IFCAP		NOIS		RUN TIME LIBRARY		
	X	DENTAL	X	IMAGING		NURSING SERVICE	X	SAGG		
	X	DIETETICS	X	INCIDENT REPORTING		OCCURRENCE SCREEN		SCHEDULING		
		DISCHARGE SUMMARY	X	INCOME VERIFICATION MATCH		ONCOLOGY		SECURITY SUITE UTILITY PACK		
	X	DRG GROUPER	X	INCOMPLETE RECORDS TRACKING	X	ORDER ENTRY/RESULTS REPORTING	X	SHIFT CHANGE HANDOFF TOOL		

(FY 2010) PIA: Minor Applications

Add any information concerning minor applications that may be associated with your system. Please indicate the name of the minor application, a brief description, and any comments you may wish to include. If you have more than 3 minor applications please copy then below sections as many times as needed.

	Name		Description		Comments
Minor app #1					
			Is PII collected by this min or application?		
			Does this minor application store PII?		
			If yes, where?		
			Who has access to this data?		

	Name		Description		Comments
Minor app #2					
			Is PII collected by this min or application?		
			Does this minor application store PII?		
			If yes, where?		
			Who has access to this data?		

	Name		Description		Comments
Minor app #3					
			Is PII collected by this min or application?		
			Does this minor application store PII?		
			If yes, where?		
			Who has access to this data?		

(FY 2010) PIA: Final Signatures

Facility Name: VA Ann Arbor Healthcare System

Title:	Name:	Phone:	Email:
Privacy Officer:	Sandra Kidd	734-845-5314	sandra.kidd@va.gov
SANDRA O KIDD Digital Signature Block	Digitally signed by: SANDRA O KIDD DN: CN = SANDRA O KIDD O = Department of Veterans Affairs OU = Dept. of Veterans Affairs, Internal Staff Date: 2010.05.14 15:23:01 -05'00'		
Information Security Officer:	Mark Latendresse	734-845-5351	mark.latendresse@va.gov
LATENDRESSE, MARK Digital Signature Block	Digitally signed by LATENDRESSE, MARK Date: 2010.05.13 11:45:00 -04'00'		
Chief Information Officer:	Ronald Wuthrich	734-845-5733	ronald.wuthrich@va.gov
Digitally signed by: RONALD A WUTHRICH DN: CN = RONALD A WUTHRICH O = Department of Veterans Affairs OU = Dept. of Veterans Affairs, Internal Staff Date: 2010.05.14 12:18:34 -05'00' Digital Signature Block			
Person Completing Document:	John M Wilkerson	734-845-5563	john.wilkerson@va.gov
JOHN WILKERSON Digital Signature Block	Digitally signed by: JOHN WILKERSON DN: CN = JOHN WILKERSON O = Department of Veterans Affairs OU = Dept. of Veterans Affairs, Internal Staff Date: 2010.05.13 11:39:50 -05'00'		
System / Application / Program Manager:	Richard Ray	734-845-3960	richard.ray@va.gov
RICHARD RAY Digital Signature Block	Digitally signed by: RICHARD RAY DN: CN = RICHARD RAY O = Department of Veterans Affairs OU = Dept. of Veterans Affairs, Internal Staff Date: 2010.05.13 13:30:18 -05'00'		

Date of Report:	4/30/2010
OMB Unique Project Identifier	029-00-01-11-01-1180-00
Project Name	Ann Arbor VA Healthcare System – VistA Legacy